USAWC STRATEGY RESEARCH PROJECT

Information Operations – Demands Of Increased Cooperation Within the Cabinet and Between the State and Private Sector

by

Colonel Ingvar Hellquist
Swedish Armed Forces

Colonel Felix Castro
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
07-04-2003		xx-xx-2002 to xx-xx-2003

4. TITLE AND SUBTITLE
Information Operations - Demands of Increased Cooperation Within the Cabinet and Between the State and the Private Sector
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Hellquist, Ingvar ; Author

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Army War College
Carlisle Barracks
Carlisle, PA17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Same as Report (SAR)	28	Rife, Dave RifeD@awc.carlisle.army.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number DSN

ABSTRACT

AUTHOR: Colonel Ingvar Hellquist

TITLE: Information Operations – Demands of Increased Co-operation Within the Cabinet and Between the State and Private Sector

FORMAT: Strategy Research Project

DATE: 07 April 2003 PAGES: 28 CLASSIFICATION: Unclassified

This paper presents a comparison between Swedish and the United States perspective on actions to reduce vulnerabilities in critical infrastructure when that infrastructure is attacked via Information Operations. It compares the U.S. and the Swedish definitions of Information Operations and offers an example of how Information Operations can be implemented. The paper stresses the need for increased co-operation among government and increased awareness of the government's needs within the economic environment. With technological advancements occurring mostly in the purviews of the private sector, no single actor is the owner of a critical information system. Yet information technology and globalization leads to the international arena and demands international co-operation. This paper suggests ways how the different actors can attain co-operation throughout a nation's critical systems. An area of special interest, because of their authority and collaboration in an asymmetric environment, is the role of police and military, in protective information operations. This paper address information operations by looking at issues of global security, technological developments and economic situations. This paper stresses the need for developed forms of public-private cooperation and describes a view of how to organize traditional domestic responsibilities to better keep pace with emerging IT-related threats. The paper also recommends new ways of handling crises and conflicts, as well as enforcing sanctions in the international arena Recommendations are provided for cross-sector security co-operation within the cabinet and between the State and private sector.

TABLE OF CONTENTS

INFORMATION OPERATIONS – DEMANDS OF INCREASED CO-OPERATION WITHIN THE CABINET AND BETWEEN THE STATE AND PRIVATE SECTOR

INTRODUCTION

This paper presents a comparisons between Swedish and the United States perspective on actions to reduce vulnerabilities in critical infrastructure when that infrastructure is attacked via Information Operations. It compares the U.S. and the Swedish definitions of Information Operations and offers an example of how Information Operations can be implemented. The paper stresses the need for increased co-operation among government and increased awareness of the government's needs within the economic environment.

With technological advancements occurring mostly in the purviews of the private sector, no single actor is the owner of a critical information system. Yet information technology and globalization leads to the international arena and demands international co-operation.

This paper suggests ways how the different actors can attain co-operation throughout a nation's critical systems. An area of special interest, because of their authority and collaboration in an asymmetric environment, is the role of police and military, in protective information operations. This paper address information operations by looking at issues of global security, technological developments and economic situations.

This paper stresses the need for developed forms of public-private cooperation and describes a view of how to organize traditional domestic responsibilities to better keep pace with emerging IT-related threats. The paper also recommends new ways of handling crises and conflicts, as well as enforcing sanctions in the international arena

Recommendations are provided for cross-sector security co-operation within the cabinet and between the State and private sector.

An increased cooperation within the State, and also between the State and its economic environment, are essentials to decrease the vulnerability of information systems important to the society in case of an attack using information operation.

THE NEED FOR COMMON ACTION

The dominant use of information technology detrimentally affects the State and its economic life when it is attacked. This is particularly true for information technology used by the military. Other critical infrastructures affected include the economic system, electrical and water supplying systems, and most particularly it affects communication and information systems.

Technology will continue its developmental progress, followed by a demand for its use in rational and effective systems. This will increase the need for the integration and joint exploitation of, among others, communication and information systems, which have become an increasingly dominant part of the operational control of the critical functions mentioned above. Communication and information systems cannot be protected on their own by their users. Rather all affected parties must cooperate buy contributing resources and knowledge while building a working defense against information attacks.

When attacks occur, striking against systems and functions important to society, huge costs and loss of benefits result. The consequences of an attack can ultimately impact on private individuals, affecting the basic foundation of their normal lives. Attacks on infrastructure endanger the country's ability to function, to continue as a law-governed society with adequate, public health, energy, communications, and military defense. The economic sector can be stricken by large economic losses and eliminated production, leading to large payments by insurance companies and mistrust of financial systems.

Each of the actors in the infrastructure has good reasons to improve its security, and already significant efforts are in progress. But self protection is not enough, since the greatest weakness lie in the fact that the systems are connected between actors.

Some of the actors have, by means of their responsibility for a particular function or their market situation, a natural commitment to improve security within, between, and among information systems. The most obvious actor is the government of the country, whose most important function is to defend the security of its citizens and a good economic environment for the economic sector. Other important actors are the producers of the many IT systems. Their credibility and their share of the market are dependent on customers being able to trust their systems. Further actors are the suppliers of data and telecommunications, for motives similar to those of the producers of IT systems. The financial institutions are also important actors when it comes to improving security within information systems.

The banking and insurance business have incentives to participate in the construction of an effective protection of information systems exceeding their own specific boundaries, as every attacks on a country's infrastructure will finally effect the branch responsible for the settlement of claims. The support of insurance companies as a partner for cooperation beyond that of its own boundaries can be counted on because their main interest is decreasing expenses caused by damage, regardless of the cause or its purpose, intentional or unintentional.

The police and the military have a special role in the infrastructure; their main task is to answer for everyone's safety. Co-operation between these two actors, however, is made difficult

when one attack on information systems occur. Whole the points of intersection between advanced criminality and war have increased, the rules and regulations now existing and imposed on actions of the police and the military were created to keep the actors separate and appropriate to only one stat of the union: war or peace.

Globalization within the commerce and economy and also the protection there of, has resulted in an increasing number of issues that cannot be nationally resolved. The prominent international collaboration is essential, to maintaining the best interests of both the State and its economic sector. One example is concerning the defense industry who in previous time was abele to provide products with domestic resources but now days are deeply depending on international provided parts and systems.

It is also important for investors how a country is viewed from outside to be respected as a safe marketplace and partner. Central Intelligence Agency (CIA), The World Fact Book, looks on Sweden in the economic area as a country that in resent year has clouded its extraordinarily favorable picture.

> By budgetary difficulties, inflation, high unemployment, and a gradual loss of competitiveness in international markets. [1]

There are many reasons for an extensive collaboration between the State and its economic sector within the field of information systems. So why does this not happen in an extent that is sufficient and why is it so difficult to find solutions that are common and comprehendible to the society, when the problem in fact is known?

SEEING THE SOLUTIONS

Information operations, along with information security and information warfare, are perceived as complex phenomena for our time. Why are they believed to generate complicated issues?

First, the techniques that make the activities and functions successful are advanced and hard to understand, despite making the use of the technique simple and user friendly. There are a large number of technical functions and inter-dependencies that are for the main part unknown to the users. There is also a wide gap between the persons who create, understand and use the technology and those that make the decisions important for the well-being of the society and its economic life.

Second, intentional attacks against information systems are hard to detect and trace. It is difficult to determine clearly at who the attack was aimed and for reason. It is hard to identify

vulnerabilities in one's systems in advance, what actions to take to improve the protection, and with whom to collaborate. Technical shortcomings, unintentional attacks, and or faulty actions by users increase the difficulty in identifying intentional attacks.

Third, neither national nor international rules and regulations are adapted to deal with technology's fast and globally widespread progression. Therefore roles have been set by the market, rather than by Parliaments.

Fourth, demarcation of areas of responsibility in information systems does not align themselves easily with the areas of responsibility traditional to society. It is particularly hard to determine what is civil, social, military or economic. This attaining a national coordination of effort is difficult to solve archive.

Fifth, it's difficult to maintain secured information systems without simultaneously developing an offensive capability. It is by natural that the creation of a system having an offensive capability does not want to share that part of its system and knowledge with others. It is too likely that an adversary might develop a defense to counter the offensive capability. Or if system knowledge would get into wrong hands it could be used against the originator or originator's nation. This developing one's own protection of information systems is obstructed.

Sixth, collecting statistics concerning IT related incidents, is an arduous task and most incidents remain undiscovered. The credibility of the informants as a company or authority can be lost when vulnerability's in their systems being displayed. Several of the reports can therefore not be recorded in a joint manner, owing to the protection of the informants personal or company integrity.

Seventh, it is a delicate effort to map circulation of false information and trace information operations in the media. Information published in the media is founded on freedom of speech and the right of society to be self-critical. Mapping information published in the media, with the aim to trace an ongoing information operation or preparations for such operation, is easily experienced as an encroachment on these rights.

WHERE IN THE PROGRESS ARE WE?

Order of security

We are presently maturing in the age of information, at least in large parts of the world. This increases the gap between rich and poor and leads to conflicts and solutions thereof that extend over a large field. But an entire continent or region cannot simply be characterized as trolling in their development. Knowledge is available world-wide, although in some countries only the elite has that knowledge.

After the fall of the Soviet Union, the war suppressing effect created by the balance of power between the two superpowers disappeared. That effect can be compared to a game of chess; when all the squares are mortgaged, no strike is possible. When local conflicts arise nowadays, no preventing circumstances exist. Instead, each conflict has to be solved with other means. The solutions of conflicts have become more dependent on international cooperation and an increasing number of actors.

The reasons for conflicts have not changed to the same extent. Remaining is the conflict concerning natural resources and their distribution. Most of the earth's population uses these valuable natural resources, and now is a hotbed for terrorism and hatred which will remain over a long period of time.

Experience with international terrorism has made us aware that the threats of our time have no respect for the borders of a country. This is especially true for threat imposed by weapons of mass destruction. During the 1990s we saw the horrible and ongoing consequences that ethnic and religious difference can lead to. Today, much of the world is aware of that poverty, oppression of human rights, organized crime, diminishing resources, streams of refuges and the spread of HIV/AIDS can threaten our shared future's security.

There are no world police. Although the United States holds a prominent position of power it is not the world's policeman. However, the conditions for being world police are based on rules and regulations of such kind that states must give up large parts of their sovereignty and influence. That this will happen in the present and ongoing future is however an unrealistic thought.

Of later years, there have been large changes in the relations ships among nations. There are many reasons for this, for example, the importance of cyber space, the exchange of knowledge between non state actors, global economy, diseases, air pollutions, global warming and international terrorism. This affects how decisions are made, national and international laws, defense collaboration, and a great deal more.

Technical development

Groundbreaking discoveries made by experts and scientists are seldom available to or understood by the generation present at the time of the breakthrough. The science of today is no exception, even though we do not fully understand were it is heading, we do understand that it will lead to major changes in the future. The ability to utilize that further knowledge and the willingness to change will separate the winners from the losers.

It is tempting to consider the technical development, enabling the use of electricity, nuclear power, computers, and even space stations as the driving force in all development. But it is likely that the more important developments are those of awareness, of ways to communicate and of ways to mediate knowledge. Take the Internet, fore example. The Internet is a very special phenomenon. The Internet is limited only by our imagination. Its importance is in its use for sharing information and for communicating. It grew with tremendous speed; its wide distribution has affected the entire world. The Internet is objective, global, swift as lightning, addictive, trend setting, true, false, without borders. The Internet is also an advanced means of giving intelligence for nations, industries, police, military, terrorists, criminals and the like. The Internet is a tool for planning, a storage area, and a gigantic billboard.

The Internet is also relatively cheap. Because users became dependent or having access to a computer and being connected to the Internet competition is generated among suppliers, which in turn results in lower cost products. The supply of inexpensive computers and Internet access makes it possible fore nearly everyone, even average citizens in less wealthy countries, to be connected to the Internet.

Economy

Money has long been one of the most important means used to reach agreement about the exchange of services and products. The power to effect the distribution of money is one of the most important empowering factors within a nation and its public sector. Today's global economy is of such importance that nations develop and apply their strictest sets of rules and regulations to methods of guaranteeing economic transactions and agreements. The market is so global that companies can have their trademark in one country, their head office in another country, their production in a third, their research and development in a forth and so on. Countries without trustworthy laws and sets of rules and regulations governing trade are uncertain marketplaces, placing them in a position leading to national economic losses for these countries.

The methods for transferring money among individuals, within and between companies and between States and organizations have changed markedly with the advent of electronic banking. The numbers of currencies that dominate the foreign exchange have decreased. There are fever people involved. The speed at which the transactions can be carried out has increased exponentially.

Conclusion

All taken together, these changes have reduced government's influence over development of its economic life and decreased its ability to ensure its country security. Both of these changes favor influence of global actors, and large organizations like the European Union (EU)and the United Nations (UN) as well as small terrorist organizations.

Local conflicts have increased. The uses of asymmetric methods to start or solve conflicts have become common. It is harder to limit conflicts to the media or to certain territories. The number of parties involved in conflicts has expanded. Modern conflicts can be pursued with everything from high technology weapons to ancient ways of using force.

The ability to resolve conflicts has become more dependent on international cooperation, which requires more international actors to become involved. The global economy is central to the development of the world. It is the motivating power that drives progress in both nations and companies, yet at the same time it is the cause of stagnation and regression for those not being able to keep up with the demands set by economic growth. It is, however, human natures to strive for knowledge and insight that, together with man's inherited need for communication, drives the world's transition to the age of information creating economic incentives and growth conditions for both the nation and its economic life.

Short-ranged oscillations in business that result from technical progress and variable consumption affect a lot of people deeply, while long-ranged economic factors, that results the availability of natural resources and the global demolition thereof, affect the market to a lesser extent. The Swedish Minister of foreign affairs described the new challenges for the world as below;

> The international order of security has changed. The concept of security has been broadened and the focus has been shifted. The geographical dimension of security loses its importance when the integration of governments and globalization of industry erase the borders between what is national and what is international security. Security today covers much more than the lack of war and conflicts between countries.[2]

WHAT IS INFORMATION WARFARE AND WHAT IS INFORMATION OPERATIONS?

Much has been written about the distinctions between Information Operations and Information Warfare. It nearly seems as if the definitions themselves are part of an information operation.

Martin C. Libicki has in his book What is Information Warfare? rejected information warfare as a separate technique of waging war. He argues instead that there are several distinct forms of information warfare, each laying claim to the larger concept, all of which, one way or another, involve the protection, manipulation, degradation, and denial of information. He further divides Information Warfare into:

- Command–and-control warfare, which strikes against the enemy's head and neck.
- Intelligence-based warfare, which consists of the design, protection and denial of information systems that seeks sufficient knowledge to dominate the battle space.
- Electronic warfare, which uses radio-electronic and cryptographic techniques to gain or deny information.
- Psychological warfare, in which information is used to change the minds of friends, neutrals, and foes.
- "Hacker" warfare, in which computer systems are attacked to obtain or destroy information.
- Economic information warfare, which blocks information or channels it to pursue economic dominance.
- Cyber warfare, which is a grab bag of futuristic scenarios. [3]

DEFINITIONS

The U.S. Department of Defense Directive (DoDD) S-3660.1 views information definitions and policy as follow:

Information Operations (IO) are actions taken to affect adversary information, information systems and decision making, while defending one's own information, information systems and decision making.

Information Warfare (IW) is Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

POLICY

The Department of Defense (DoD) supports the national security strategy and national objectives through the accomplishment of a variety of missions that range across the spectrum of military operations from peace to war. In peacetime the DoD conducts activities to accomplish these missions and shape the international environment. In conflict, as in peacetime, information superiority enables the DoD to direct the full power of Information Age concepts and

technologies, transforming capabilities for maneuver, strike, logistics, protection and situation awareness into full spectrum dominance.

A primary focus of IO (defensively and offensively) is ultimately on decision-makers; the information they acquire and use to make decisions, the information they generate in making decisions and the full range of systems and organizations involved in handling, processing and implementing this information. IO may also be used to effect the automated component of a weapon system.

Information Operations, conducted as an integral element of land, sea, air, space, special and joint operations, contributes to information superiority by protecting military decision-making from adversary attacks and, as necessary, degrades an adversary's decision-making, thereby producing a relative information advantage.

One set of IO activities employed by the DoD Components focuses on the perceptions and attitudes of decision-makers or groups. A second set of IO activities also employed by the DoD Components focuses on attacking or defending the electromagnetic spectrum, information systems, and information which supports decision makers, command and control and automated responses.

> The DoD's activities to conduct IO include psychological operations (PSYOP), electronic warfare (EW) (including directed energy), computer network operations (CNO), information assurance (IA), military deception, security, and counterintelligence. [4]

CONCEPT AND DEFINITIONS FROM A SWEDISH PERSPECTIVE

The concept starts from a top-down, national security perspective, rather than from a bottom-up information security perspective. This perspective suggests a holistic approach to information operations. In the Swedish Defense Bill from November 1999 (Swedish Ministry of Defense 1999a), the Cabinet described the matter as follows:

> The threat against the information society has become increasingly important at the same time as systems and functions important to the society are becoming more dependent on information technology. The question of society's vulnerability in this respect has a strong bearing on security policy. [5]

Accordingly, Swedish substantive definitions adhere to the taxonomy defined by the US (JP 3-13, Joint Chiefs of Staff (US), 1998), and later also adopted by NATO, where IO is the comprehensive term. Information Operations could be offensive or defensive and incorporates

more than IT-related matters, including intelligence, perception management, operational art, etc, within a strategic context.

Information Assurance (IA) is the Information Technology related foundation within the term IO. It could be seen as the highest level for the bottom-up perspective where organizations and policy have been added to the traditional information security toolbox.

With this top-down perspective and the long-standing Swedish tradition of a Total Defense concept, where all-important functions in society are included in the event of crisis/war, it is more logical to talk about the wider term Defensive Information Operations (IO-D) than just Information Assurance.

INFORMATION OPERATIONS AS AN EFFECTIVE WAY TO ATTACK – EXAMPLE

Because of the confusion, created by variations in definitions, and different wives of what could happen when a nation conducts an information operation to another nation, it could be useful to discuss offensive actions and defensive protection by study an example. This example is therefore beyond intrusions in information systems conducted by hackers and terrorists groups.

Take country A, a victim and target in this example of an information operation. Country A has high-technology industry, economic prosperity and a well-serving democracy. Its national security is built upon principles formed by relations among states in the present world order. Country A has strong military defense forces capable to defend its borders and its territory. It utilizes advanced technology equipment and modern control and command-system. Built on experience from the second world-war, and from the following cold-war period, the society is well prepared to reject a military aggression. The law-system, and demands on agencies in wartime are genuine established.

Country A maintains a very strict barrier between military and law enforcement agencies. Military resources can, during peacetime, only assist in rescue efforts. Also within the intelligence-sector is the barrier sharp. Its economic life and its government both have a strong interest in maintaining a sable market economy. The effects of global economy and the strong feature of multinational companies in the country imply that investment more often is in favor of increased share of the market than in security.

Another, Country B, the aggressor-country, is motivated to attack Country A to gain natural resources and material for producing weapons of mass destruction. This aggressor nation is in cooperation with a terrorist organization, Dead Team. Dead Team has cells in many countries.

After a period of political tension between the countries a military confrontation takes place, caused by a military ship from Country B sinking a refuge boat from Country B in the territorial waters of Country A. Military readiness increases in both countries. The political epilogue results in frozen diplomatic relations between the countries.

An other incident a bomb detonates among the spectators at a sport event in Country A one week after the sinking of the boat. Almost 400 of the spectators are killed. They are mainly from Country B. No nation or organization claims the bombing, but evidence points to the Dead Team.

One month later a hurricane sweeps over Country B. Aquatown, a city near the coast is devastated. Country B is strongly dependent on fresh water from Aquatown and that water supply has become contaminated. Aquatown was the economic center of the country B.

It is critical for Country B to get access to uranium. Its nuclear power station is running out of fuel because neighboring Country C has prevented delivery of uranium since Country B started exploring nuclear weapons. There are no UN-resolutions about this issue. Country B feels threatened and suffers after the hurricane and tries to obtain uranium from Country A. Country A feels the same tension as Country C and refuses to sell any uranium.

During the next six months the situation gradually worsens for Country B. The government decides to use information operations to attack Country A to obtain uranium and water from a common river. Country B demanded a huge amount of money to rebuild Aquatown. The operation-planning is conducted by the military headquarters with Dead Team members through a secret pact.

Within the military headquarters there is an information warfare cell. In this cell some of the world-leading hackers have been enlisted. They have succeeded in developing a destructive software virus and have inserted it in Microsoft software products. The virus is released through license-holders via the Internet. This virus makes it possible to access bank security systems.

The attack starts when deluding information about corruption within the government is given to the media. The attack includes intrusion in the election systems. Voting-results are manipulated in such number that the Cabinet no longer is held by the majority party. The speaker of Parliament announces the last election invalid. Planted evidence that supports the crop of rumors about corruption is found in the banking-system. Preliminary investigations are initiated against the Prime Minister.

Country B’s hackers purposely hide their connection to Country B in order to confuse Country A in finding any evidence that Country B is behind the attacks. Computers of

companies and private persons in various sectors of the society have been affected by the virus. Backtracking of the attacks end up in different IP-addresses all over the world.

Country B's operation plan included a coordinated attack on electric plants, water supplies, and media by paralyzing these critical natural targets via intrusion in the IT-systems. The next phase would be to physically destroy critical centers for electricity generation and water supply. To prevent repairs of any damage, snipers and personal mines would be placed around these resources. In addition country A's water would be polluted with organisms causing epidemic cholera.

Country B wants to force an ultimatum concerning the uranium, money and water rights of the river it holds in dispute. If Country A doesn't meet the demands, Country B intends to take military actions.

Possible consequences in country A and suggestions of preemptive actions

During those circumstances, as given in the example above, there are many reasons to believe that Country A will succumb to Country B's demand. The national damage caused by attacks on the infrastructure and information-systems, and the population's distrust to its national leadership would lead to tremendous national difficulties and economic stagnation. The possibilities to gain international support beyond humanitarian operations are limited.

The financial damage, caused by the lack of a security system and information assurance in Country A can lead to economic demands to, both domestic and international, cover of losses. Country A and its economic life will be less trusted. Business and cooperation will decrease. The fact that Country B probably will face strong international critic and sanctions may be a poor consolation for the inhabitants in country A.

Among the preventive security-measures that can be accomplished is the development of new technical systems; this is the most common move. The optimal action is to engage complete cooperation among owners of critical systems and gain their adherence to whatever security mechanism is under development.

Military defense institutions have developed into a complicated network-based organization, more and more dependent on private industry. New security structures are created due to high-security demands put on the military. The same motive power does not exist within remaining sectors of the society to invest in security when economic resources are limited. Because of that it will be necessary to use cross-sector security solutions to reach a higher collective security.

One way to structure the security is to prioritize common systems and use layered security. One example of how limited access is provided is intranet. They are more restricted than the Internet in connecting to other networks. Another example is the separation between a customer doing Web-banking and a more secure system within the banking systems completing the transactions. These examples could be models of how to reach higher protection and security in the most sensitive information technology systems in the critical infrastructure.

Another example is from the U.S. It is a network administered by the Federal Bureau of Investigation (FBI) to share security information. It was started in 1996 to create collective security among states and the private sector and is named INFRAGARD. [6] Infragard obtains further approval in efficiency when President Bill Clinton issued Presidential Decision Directive (PDD 63) to increase security within the critical infrastructure area.

A COMPARISON OF SWEDEN AND THE US IN DEFENSIVE INFORMATION OPERATIONS AND CRITICAL INFRASTRUCTURE PROTECTION

There are differences between the management models endorsed by the U.S. Government and those of Sweden. A major emphasis on the new IO-D semi-independent coordinating body remains within the Swedish Emergency Management Agency (SEMA). This body is the equivalent to the Critical Infrastructure Assurance Office (CIAO) with its planning responsibilities, but it also comprises the threat and intelligence functions that in the U.S. belong to the United States National Infrastructure Protection Center (NIPC). Secondly, the Swedish Gov-CERT could be seen as a NIPC, but less responsible, with just the warning and tracing roles. This function has been put under the auspices of the Post- and Telecommunications Agency, due to its legal mandate over civilian networks. Law enforcement officers are detached to the Gov-CERT. In the U.S. the function is reversed with the NIPC and the Federal Bureau of Investigation (FBI).

A significant advantage for Sweden compared to other countries is The Private Sector's Security Delegation to do its public-private security co-operation. This case is like a one-stop-shop for the government to co-operate with the private sector. The least common denominator is for politicians and industrialists to join forces against emerging IT-threats, described as "Sweden should be a safe and secure marketplace!"

Sweden has taken a holistic approach, actively involving a wide spectrum of national and international organizations like the United Nations (UN) and Interpol, to solve the IO problem. Another example is its active support of international agreements and regulations designed to facilitate rapid tracking across national borders. In these cases, the G-8 Committee has produced recommendations and the Council of Europe has also endorsed these.

The issue of responsibilities is somewhat complex in Sweden as the constitution has a 350-year-old heritage of small Cabinet Departments and strong, independent agencies. This goes back to the 17th century, when King Gustaf II Adolf was out in Europe for long campaigns during the Thirty Years' War. He wanted a stable government that could run domestic business without his immediate presence. The agencies are formally subordinated only to collective Cabinet decisions (at least five ministers present) - not to the minister concerned or the Cabinet Department. This governmental system, with its strict sector boundaries, great authority for the Director-Generals, weak ministerial authority and no formal interagency coordination body, is not so well-suited to take care of the new cross-sector threats in the Information Age.

In September 1999 the Defense Commission, comprised of parliamentarians on a DoD assignment, published a white paper (Swedish Ministry of Defense, 1999c) which proposed guidelines on National Security and Defense for the next five years. This paper addressed IO issues in the round - from the urgent need for restructured domestic cooperation between joint military and civilian parts of the Total Defense concept, to the need for international co-operation. The white paper concluded that the question of vulnerabilities in Swedish society was "of great importance to security policy." [7]

INTERNATIONAL COOPERATION AND INTERNATIONAL LAW

In today's world asymmetrical warfare is a reality, and the thoughts of Sun Zu (500 BC) have been reinforced. Aggressors, terrorists, advanced criminals and hackers will always try to exploit societal vulnerabilities at their weakest point.

The protection against the aggressors often leads to increased state-control. The impact of state-control on its citizens, relations to other countries, international law and human rights are essential.

The events of September 11 2001 led to "The Global War on Terrorism," which became a united effort among most nations. Tolerance about state violations of private and human rights were almost universally accepted. It was understandable due to the fear of terrorism and the will to join the world community against this terrible threat. Now more than a year has passed.

According to The National Security Strategy of the United States presented in September 2002;

> The United States must and will maintain the capability to defeat any attempt by an enemy – whether a state or non-state actor - to impose its will on United States, our allies, or our friends. [8]

This statement challenges the established relationship of state-to-state that has served the world since the 17th century. To compare actions made by non-state actors with states, and to deal with these actors with the same means as used in war against states, changes the world-order.

There have already been some international reactions against parts of U.S. policy. One was when Al-Qaida prisoners were sent from Afghanistan to the U.S. base at Guantanamo, Cuba. The fact that U.S. prosecuted these prisoners using war-laws was in strict contrast to what most nations thought appropriate. Compared to normal law enforcement, the quality of evidence is lower, and trials are not conducted in public. And due to the fact that prisoners had different nationality and citizenship, agreements concerning exchanges of prisoners between countries were violated.

Another was, at least in Europe, when the U.S. rejected agreements on prosecuting potential U.S. war criminals in the international court. There is a real concern about what the result could be if the U.S. on one hand asks for united cooperation against terror and on the other hand does not act in the same way if terror were to be conducted by U.S. soldiers. There is a way to reduce this kind of friction, but it would mean a change in U.S. policy. The National Security Strategy of the United States continues;

> Ultimately, the foundation of American strength is at home. It is in the skills of our people, the dynamism of our economy and resilience of our institutions. A diverse, modern society has inherent, ambitious, entrepreneurial energy. That is where our national security begins. [9]

Domestically within the U.S. there are several problems to face when stronger methods are used to prevent terrorists attacks and to find terrorists after an attack. The freedom of movement, the right of privacy, and understanding among different groups of people, as stated above, are deeply founded in American culture and society.

When three young men were arrested in Florida, after a very thin tip-off concerning some conversation among them about terror, and later released because of lack of evidence it was the beginning of a debate about the future legal system in the USA. The sniper-case in Maryland gives also points to consider about coordination of intelligence and assembling individual-related facts in some central register.

There have been increasing changes in the U.S. in the way individuals are tracked, registered and investigated by authorities. There are also signs of isolation by enforcing higher requirements to be able to visit or immigrate into the U.S. Both these trends will, if they

continue, change the American lifestyle in a direction at odds with the ongoing globalization in the world.

One issue, on the defensive side of information operations, is that increased international co-operation becomes necessary for improving the possibilities of making trace-backs in near real time. If an attack occurs on a country's information system originating outsides its borders, it could take several days to pinpoint the attack and to learn more on the whereabouts of the perpetrator. The attacked victim have to contact the police in its country who in turn would make contact with the police authorities in other countries from which the attack has been determined to come and negotiate assistance from them. It is therefore important to provide active support for international agreements and regulations designed to facilitate rapid tracing across national borders.

At the 53rd meeting of the United Nations General Assembly (December 1998), a resolution (UNGA 53/70) proposed by Russia was – after some modifications from U.S. and other countries - unanimously adopted to the effect that the threat to civil information systems. The threat could emanate from terrorists and criminal groups and be heeded by the international community and cross-border measures implemented. Continuing discussion of this topic prior to this year's General Assembly resulted in the need for bilateral as well as multilateral (UN, Interpol) contacts to emerge.

The political view formed by the Swedish Cabinet in November 1999 and approved by the Parliament in May 2000 stressed the need for a revision of International Law in this respect.

> The use of cyber-weapons to attack information systems does not constitute violence in terms of international law but it may nevertheless contravene international law. At the same time it should be possible to make use of such weapons within the provision of the UN Charter (Article 41) given an appropriate UN Resolution and consequent legal mandate in order to uphold sanctions or for other conflict prevention measures even though this has hitherto not happened.[10]

There are no borders in cyberspace and governments must be able to cope with criminals and terrorists in cross-border IT-activities. The international community should strengthen their collaboration efforts to enforce "smart sanctions" against rogue states. The need for international cooperation is obvious.

RECOMMENDATIONS

Serious threats against democratic states exist in the crossing-point between advanced criminality and war. Vulnerabilities in our high-tech and modern society are the foremost challenge to national security. This serves as the starting-point in a modern security strategy and for serving crisis management institutions. There are new demands to form and develop a new protection of the society. The lack of capability to cooperate or take advantage of the recourses in society has cost the taxpayers a tremendous amount of money. Even more serious is the lack of efficiency in urgent crisis management.

In February 2003 the chairman of The Swedish Defense Commission [11] gave a speech about national security and how national coordination can be achieved.

> We need a committee concerning vulnerabilities and security in Parliament and a commend handling of politicians from especially department of trade- and commerce, of justice and department of defense. It would increase the possibilities to find overlapping solutions in the security-area. The interest of the citizens would be placed above the interest to protect the different sectors. [12]

The new crisis management should consist of coordinated civil-military crisis management structure that is responsible for command and control of territorial integrity; critical infrastructure protection; information operations; and intelligence. The mandate for The Swedish Emergency Management Agency (SEMA) should be expanded. The joint command should be an operational part of the cabinet.

To be able to achieve some of what The Swedish Defense Commission is asking for there must be created an IO network in which members from the Cabinet, law enforcement, the Emergency Management Agency (SEMA), insurance sector, banking sector, IT- consults, military defense, intelligence agencies, national companies of importance and some other actors, depending on developments in the area, are participants.

WORD COUNT = 7402

ENDNOTES

[1] Central Intelligence Agency (CIA), The World Fact Book 2001, Washington, D.C.: Central Intelligence Agency, 2001), 477.

[2] Anna Lindh, Minister of Foreign Affairs, Sweden. "Säkerhetspolitiken och folkrätten - våra utmaningar idag." (Speech given in Sälen, Sweden on 19 January 2003). Available from <http://www.cff.se/verksanhet/talsalen2003/talsalen03.html>; Internet; accessed 19 January 2003.

[3] Martin C. Libicki, What Is Information Warfare? (Washington D.C.: National Defense University Press, August 1995),7.

[4] U.S. Department of Defense. Available from <http://cryptome.org/dodd3600-1.htm>; Internet; accessed 20 February 2003.

[5] Swedish Ministry of Defense (1999a) The New Defense, Bill to Parliament (99/00:30) (Stockholm, 1999).

[6] U.S. Federal Bureau of Investigation (FBI) et al, "Infragard"; available from <http://www.infragard.net>; Internet, accessed 20 February 2003.

[7] Swedish Ministry of Defense (1999c) European Security –Sweden's Defense, Report from Defense Commission (Ds.1999/55). (Stockholm, 1999).

[8] White House. The National Security Strategy of the United States, (Washington, D.C. September 2002), 30.

[9] Ibid., 31.

[10] Swedish Ministry of Defense (1999a) The New Defense, Bill to Parliament (99/00:30) (Stockholm, 1999).

[11] The Swedish Defense Commission is a forum for consultations between representatives of the Government and representatives of the political parties of Parliament concerning the long-range development of Swedish Defense and Security Policy.

[12] Håkan Juholt, Chairman of The Swedish Defense Commission. "Den nya krisberedskapen - vad behöver vi ändra på." (Speech given in Sälen, Sweden on 20 January 2003). Available from <http://www.cff.se/verksanhet/talsalen2003/talsalen03.html>; Internet; accessed 20 January 2003.

BIBLIOGRAPHY

Cabinet Working-Group on Defensive Information Warfare. "Report No 2 - Measures And Protection Against Information Warfare - a Proposal for Division of Responsibilities etc." 1998. Available from <http://www.fhs.mil.se/utb/operativa/opi/ikk_eng.htm>. Internet. Accessed 14 Dec 2003.

Central Intelligence Agency (CIA). The World Fact Book 2001. Washington, D.C.: 2001.

Copeland, Thomas E. ed, The Information Revolution and National Security. Carlisle: U.S. Army War College, Strategic Studies Institute, August 2000.

Grove, Gregory D. Seymour E. Goodman and Stephen J. Lukasik. "Cyber Attacks and International Law." Survival. 42, no.3 (2000): 89-103.

Juholt, Håkan, Chairman of The Swedish Defense Commission. Den nya krisberedskapen - vad behöver vi ändra på." (Speech given in Sälen, Sweden on 20 January 2003). Available from <http://www.cff.se/verksanhet/talsalen2003/talsalen03.html>; Internet; accessed 20 January 2003.

Libicki, Martin C., What is Information Warfare? Washington, D.C.: National Defense University Press, August 1995.

Lindh, Anna, Minister of Foreign Affairs, Sweden. "Säkerhetspolitiken och folkrätten - våra utmaningar idag." (Speech given in Sälen, Sweden on 19 January 2003). Available from <http://www.cff.se/verksanhet/talsalen2003/talsalen03.html>; Internet; accessed 19 January 2003.

Nicander, Lars. Information Operations – A Swedish View." Journal of Information Warfare. 1, no. 1: (2001): 5-22.

Perry, Walter, Robert W. Button, Jerome Bracken, Thomas Sullivan, and Jonathan Mitchell. "Measures of Effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Outcomes." Available from <http://www.rand.org/publications/MR/MR1449/>. Internet. Accessed 17 January 2002.

Pumphrey, Carolyn W. ed, Transnational Threats: Blending Law Enforcement and Military Strategies. Carlisle: U.S. Army War College, Strategic Studies Institute, November 2000.

Stuart, Douglas T. ed, Organizing for National Security. Carlisle: U.S. Army War College, Strategic Studies Institute, November 2000.

Swedish Cabinet Bill. The New Defense (1999/2000:FöU2). (Excerpt, unofficial translation). Available from <http://www.fhs.mil.se/utb/operativa/opi/ikk_eng.htm>. Internet. Accessed 8 January 2003.

Swedish Ministry of Defense (1999a). The New Defense, Bill to Parliament (99/00:30). Stockholm: 2000.

Swedish Ministry of Defense (1999b). A Changed World – A Reformed Defense. Bill to Parliament (98/99:74). Stockholm: 1999.

Swedish Ministry of Defense (1999c). European Security - Sweden's Defense, Report from the Defense Commission (Ds.1999/55). Stockholm: 1999.

Swedish National Defense College. Available from <http://www.fhs.mil.se/institut/kvi/cios/english/index.html>. Internet. Accessed 14 December 2002.

Swedish Parliament (2000). Comment from The Defense Committee on Information Operations – A Swedish View. Stockholm: 2000.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, D.C.: 1998.

U.S. Federal Bureau of Investigation (FBI) et al. "Infragard." Available from <http://www.infragard.net>; Internet. Accessed 20 February 2003.

White House. National Security Strategy of the United States. Washington, D.C.: September 2002.